EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp

L1	635	713/156.ccls.	US-PGPUB;
			USPAT;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2006/03/18 17:24

L2	577	713/153.ccls.	US-PGPUB;
			USPAT;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2006/03/18 17:24

L3	534	(713/171).CCLS.	US-PGPUB;
			USPAT;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2006/03/18 17:24

L4	296	(713/169).CCLS.	US-PGPUB;
			USPAT;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2006/03/18 17:24

L5	1120	(380/28).CCLS.	US-PGPUB;
			USPAT;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2006/03/18 17:24

L6	4	5 and (crypto near engine)	US-PGPUB;
			USPAT;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2006/03/18 17:25

L7	379	(380/278).CCLS.	US-PGPUB;
			USPAT;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2006/03/18 17:25

L8	213	(380/283).CCLS.	US-PGPUB;
			USPAT;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2006/03/18 17:25

Home | Login | Logout | Access Information | Alerts |

Welcome United States Patent and Trademark Office

Search Results

BROWSE SEARCH IEEE XPLORE GUIDE

Results for **"((crypto engine)<in>metadata)"**
Your search matched **5** of **1328352** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

e-mail

» Search Options

View Session History

New Search

Modify Search

((crypto engine)<in>metadata) Search

□ Check to search only within this results set

Display Format: ● Citation ○ Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

view selected items **Select All** **Deselect All**

□ 1. **Hardware support for high performance, intrusion- and fault-tolerant syst**
Saggese, G.P.; Basile, C.; Romano, L.; Kalbarczyk, Z.; Iyer, R.K.;
Reliable Distributed Systems, 2004. Proceedings of the 23rd IEEE Internationa
18-20 Oct. 2004 Page(s):195 - 204
Digital Object Identifier 10.1109/RELDIS.2004.1353020
AbstractPlus | Full Text: PDF(502 KB) **IEEE CNF**
Rights and Permissions

□ 2. **Design of a reconfigurable AES encryption/decryption engine for mobile**
Pionteck, T.; Staake, T.; Stiefmeier, T.; Kabulepa, L.D.; Glesner, M.;
Circuits and Systems, 2004. ISCAS '04. Proceedings of the 2004 International
Volume 2, 23-26 May 2004 Page(s):II - 545-8 Vol.2
AbstractPlus | Full Text: PDF(261 KB) **IEEE CNF**
Rights and Permissions

□ 3. **UICE: a low-power high-speed cryptographic module for RFID and embec**
Kaiser, U.;
Circuit Theory and Design, 2005. Proceedings of the 2005 European Conferen
Volume 2, 28 Aug.-2 Sept. 2005 Page(s):II/189 - II/192 vol. 2
Digital Object Identifier 10.1109/ECCTD.2005.1523025
AbstractPlus | Full Text: PDF(109 KB) **IEEE CNF**
Rights and Permissions

□ 4. **Design and test of a scalable security processor**
Chih-Pin Su; Chen-Hsing Wang; Kuo-Liang Cheng; Chih-Tsun Huang; Cheng-
Design Automation Conference, 2005. Proceedings of the ASP-DAC 2005. Asi Pacific
Volume 1, 18-21 Jan. 2005 Page(s):372 - 375 Vol. 1
Digital Object Identifier 10.1109/ASPDAC.2005.1466191
AbstractPlus | Full Text: PDF(266 KB) **IEEE CNF**
Rights and Permissions

□ 5. **Integrated design of AES (Advanced Encryption Standard) encrypter and**
Chih-Chung Lu; Shau-Yin Tseng;
Application-Specific Systems, Architectures and Processors, 2002. Proceedinc International Conference on
17-19 July 2002 Page(s):277 - 285
Digital Object Identifier 10.1109/ASAP.2002.1030726

AbstractPlus | Full Text: PDF(332 KB) IEEE CNF
Rights and Permissions

Help Contact Us Privacy & :

PORTAL
USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

crypto engine

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used crypto engine

Found **10,366** of **171,143**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale □ ▤ ▥ ▦ ■

1 High Efficiency Counter Mode Security Architecture via Prediction and Precomputation
Weidong Shi, Hsien-Hsin S. Lee, Mrinmoy Ghosh, Chenghuai Lu, Alexandra Boldyreva
May 2005 **ACM SIGARCH Computer Architecture News , Proceedings of the 32nd Annual International Symposium on Computer Architecture ISCA '05**, Volume 33 Issue 2
Publisher: IEEE Computer Society, ACM Press
Full text available: pdf(1.37 MB) Additional Information: full citation, abstract, index terms

Encrypting data in unprotected memory has gained much interest lately for digital rights protection and security reasons. Counter Mode is a well-known encryption scheme. It is a symmetric-key encryption scheme based on any block cipher, e.g. AES. The schemeýs encryption algorithm uses a block cipher, a secret key and a counter (or a sequence number) to generate an encryption pad which is XORed with the data stored in memory. Like other memory encryption schemes, this method suffers from the inhe ...

2 Embedded applications: AES and the cryptonite crypto processor
Dino Oliva, Rainer Buchty, Nevin Heintze
October 2003 **Proceedings of the 2003 international conference on Compilers, architecture and synthesis for embedded systems**
Publisher: ACM Press
Full text available: pdf(346.09 KB) Additional Information: full citation, abstract, references, index terms

CRYPTONITE is a programmable processor tailored to the needs of crypto algorithms. The design of CRYPTONITE was based on an in-depth application analysis in which standard crypto algorithms (AES, DES, MD5, SHA-1, etc) were distilled down to their core functionality. We describe this methodology and use AES as a central example. Starting with a functional description of AES, we give a high level account of how to implement AES efficiently in hardware, and present several novel optimizations (whic ...

Keywords: AES, architecture, cryptography, high-bandwidth, high-speed, processor, round key generation, software implementation

3 Computer architecture: A 3.84 gbits/s AES crypto coprocessor with modes of operation in a 0.18-μm CMOS technology
Alireza Hodjat, David D. Hwang, Bocheng Lai, Kris Tiri, Ingrid Verbauwhede
April 2005 **Proceedings of the 15th ACM Great Lakes symposium on VLSI**

Publisher: ACM Press
Full text available: pdf(283.76 KB) Additional Information: full citation, abstract, references, index terms

In this paper an AES crypto coprocessor that is fabricated using a 0.18-μm CMOS technology is presented. This crypto coprocessor performs the AES-128 encryption in both feedback and non-feedback modes of operation. A maximum throughput of 3.84 Gbits/s is achieved at a 330 MHz clock frequency for ECB, OFB, and CBC modes of operation. This crypto coprocessor can be programmed using the memory-mapped interface of an embedded CPU core and is tested using a LEON 32-bit (SPARC V8) processor in th ...

Keywords: ASIC, FPGA, VLSI, advanced encryption standard (AES), crypto-processor, cryptography, hardware architectures, security

4 Architectures for cryptography and security applications: A side-channel leakage free coprocessor IC in 0.18μm CMOS for embedded AES-based cryptographic and biometric processing
K. Tiri, D. Hwang, A. Hodjat, B. Lai, S. Yang, P. Schaumont, I. Verbauwhede
June 2005 **Proceedings of the 42nd annual conference on Design automation**
Publisher: ACM Press
Full text available: pdf(2.92 MB) Additional Information: full citation, abstract, references, index terms

Security ICs are vulnerable to side-channel attacks (SCAs) that find the secret key by monitoring the power consumption and other information that is leaked by the switching behavior of digital CMOS gates. This paper describes a side-channel attack resistant coprocessor IC and its design techniques. The IC has been fabricated in 0.18μm CMOS. The coprocessor, which is used for embedded cryptographic and biometric processing, consists of four components: an Advanced Encryption Standard (AES) ...

Keywords: countermeasure, differential power analysis, encryption, security IC, side-channel attack, smart card

5 Securing Mobile Appliances: New Challenges for the System Designer
Anand Raghunathan, Srivaths Ravi, Sunil Hattangady, Jean-Jacques Quisquater
March 2003 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 1 DATE '03**
Publisher: IEEE Computer Society
Full text available: pdf(257.28 KB) Publisher Site
Additional Information: full citation, abstract, index terms

As intelligent electronic systems pervade all aspects of our lives, capturing, storing, and communicating a wide range of sensitive and personal data, security is emerging as a critical concern that must be addressed in order to enable several current and future applications. Mobile appliances, which will play a critical role in enabling the visions of ubiquitous computing and communications, and ambient intelligence, are perhaps the most challenging to secure ¿ they often rely on a public mediu ...

6 Security in embedded systems: Design challenges
Srivaths Ravi, Anand Raghunathan, Paul Kocher, Sunil Hattangady
August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3
Publisher: ACM Press
Full text available: pdf(3.67 MB) Additional Information: full citation, abstract, references, index terms, review

Many modern electronic systems---including personal computers, PDAs, cell phones, network routers, smart cards, and networked sensors to name a few---need to access, store, manipulate, or communicate sensitive information, making security a serious concern in their design. Embedded systems, which account for a wide range of products from the electronics, semiconductor, telecommunications, and networking industries, face some of the most demanding security concerns---on the one hand, they are oft ...

Keywords: Embedded systems, architecture, authentication, battery life, cryptographic algorithms, decryption, encryption, hardware design, processing requirements, security, security attacks, security protocols, tamper resistance

7 A public-key based secure mobile IP
John Zao, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra, Stephen Kent
October 1999 **Wireless Networks**, Volume 5 Issue 5
Publisher: Kluwer Academic Publishers
Full text available: pdf(255.65 KB) Additional Information: full citation, references, citings, index terms

8 A public-key based secure mobile IP
John Zao, Stephen Kent, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra
September 1997 **Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking**
Publisher: ACM Press
Full text available: pdf(1.95 MB) Additional Information: full citation, references, citings

9 Power modeling and optimization for embedded systems: Energy-efficient data scrambling on memory-processor interfaces
Luca Benini, Angelo Galati, Alberto Macii, Enrico Macii, Massimo Poncino
August 2003 **Proceedings of the 2003 international symposium on Low power electronics and design**
Publisher: ACM Press
Full text available: pdf(147.39 KB) Additional Information: full citation, abstract, references, index terms

Crypto-processors are prone to security attacks based on the observation of their power consumption profile. We propose new techniques for increasing the non-determinism of such profile, which rely on the idea of introducing randomness in the bus data transfers. This is achieved by combining data scrambling with energy-efficient bus encoding, thus providing high information protection at no energy cost.Results on a set of bus traces originated by real-life applications demonstrate the applicabil ...

Keywords: bus encoding, data scrambling, power attacks

10 Securing ATM networks
Shaw-Cheng Chuang
January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(1.53 MB) Additional Information: full citation, references, citings, index terms

11 Research papers III: Comparative performance analysis of mobile runtimes on Intel XScale® technology
Jason Domer, Murthi Nanja, Suresh Srinivas, Bhaktha Keshavachar
June 2004 **Proceedings of the 2004 workshop on Interpreters, virtual machines and emulators**
Publisher: ACM Press
Full text available: pdf(226.94 KB) Additional Information: full citation, abstract, references, index terms

Mobile Runtime Environments such as Java*2 Micro Edition (J2ME*) and Microsoft WinCE.NET* Compact Framework* are becoming standard managed application execution environments on memory constrained devices. A variety of implementations exists, and so too are a variety of systems they could run on, and finally a variety of workloads. It becomes important to understand how they compare.In this paper we describe comparative performance analysis of mobile runtimes on products with Intel XScale® mi ...

12 APL.NET encryption HOWTO
Vladimir Kutinsky
March 2004 **ACM SIGAPL APL Quote Quad**, Volume 34 Issue 2
Publisher: ACM Press
Full text available: pdf(233.13 KB) Additional Information: full citation, abstract, references

The article outlines the key points of building a Dyalog APL interface to the GNU Privacy Guard (GnuPG), a tool for cryptographic privacy and authentication. The main purpose of the interface is to use the GnuPG's functionality to encrypt data and create digital signatures directly from APL programs. The article briefly describes .NET classes that form the core of the interface and provide effective means to manage processes running on a computer. It also contains a number of examples demonstrat ...

13 Session S4.2: program transformation: Leakage-proof program partitioning
Tao Zhang, Santosh Pande, Andre dos Santos, Franz Josef Bruecklmayr
October 2002 **Proceedings of the 2002 international conference on Compilers, architecture, and synthesis for embedded systems**
Publisher: ACM Press
Full text available: pdf(231.35 KB) Additional Information: full citation, abstract, references, citings, index terms

Due to limited available memory (of the order of Kilobytes) on embedded devices (such as smart cards), we undertake an approach of partitioning a whole program. The program partitions are down-loaded from the server on demand into the embedded device just before execution. We devise a novel method of partitioning the code and data of the program such that no information regarding the control flow and behavior of the program is leaked out. In other words, by observing the program partitions that ...

Keywords: mobile code, multi-application smart card, program partitioning, tamper-resistance

14 Workshop on architectural support for security and anti-virus (WASSA): ChipLock: support for secure microarchitectures
Taeho Kgil, Laura Falk, Trevor Mudge
March 2005 **ACM SIGARCH Computer Architecture News**, Volume 33 Issue 1
Publisher: ACM Press
Full text available: pdf(256.52 KB) Additional Information: full citation, abstract, references, index terms

The increasing need for security has caused system designers to consider placing some security support directly at the hardware level. In fact, this is starting to emerge as an important consideration in processor design, because the performance overhead of supporting security in hardware is usually significantly lower than a complete software solution. In this paper, we investigate integrating some security support into hardware. We show that security support can be added at some acceptable cos ...

15 Copyrights and access-rights: Experiences with the enforcement of access rights extracted from ODRL-based digital contracts
Susanne Guth, Gustaf Neumann, Mark Strembeck
October 2003 **Proceedings of the 3rd ACM workshop on Digital rights management DRM '03**
Publisher: ACM Press
Full text available: pdf(241.29 KB) Additional Information: full citation, abstract, references, citings, index terms

In this paper, we present our experiences concerning the enforcement of access rights extracted from ODRL-based digital contracts. We introduce the generalized *Contract Schema* (CoSa) which is an approach to provide a generic representation of contract information on top of rights expression languages. We give an overview of the design and implementation of the xoRELInterpreter software component. In particular, the xoRELInterpreter interprets digital contracts that are based on rights exp ...

16 Novel approaches: High-speed I/O: the operating system as a signalling mechanism
Matthew Burnside, Angelos D. Keromytis
August 2003 **Proceedings of the ACM SIGCOMM workshop on Network-I/O convergence: experience, lessons, implications**
Publisher: ACM Press
Full text available: pdf(127.65 KB) Additional Information: full citation, abstract, references, index terms

The design of modern operating systems is based around the concept of memory as a cache for data that flows between applications, storage, and I/O devices. With the increasing disparity between I/O bandwidth and CPU performance, this architecture exposes the processor and memory subsystems as the bottlenecks to system performance. Furthermore, this design does not easily lend itself to exploitation of new capabilities in peripheral devices, such as programmable network cards or special-purpose h ...

Keywords: Architecture, Data Streaming, Operating Systems

17 Risks to the public in computers and related systems
Peter G. Neumann
September 1996 **ACM SIGSOFT Software Engineering Notes**, Volume 21 Issue 5
Publisher: ACM Press
Full text available: pdf(927.05 KB) Additional Information: full citation, index terms

18 Tuning garbage collection for reducing memory system energy in an embedded java environment
G. Chen, R. Shetty, M. Kandemir, N. Vijaykrishnan, M. J. Irwin, M. Wolczko
November 2002 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 1 Issue 1
Publisher: ACM Press
Full text available: pdf(740.23 KB) Additional Information: full citation, abstract, references, citings, index terms

Java has been widely adopted as one of the software platforms for the seamless integration of diverse computing devices. Over the last year, there has been great momentum in adopting Java technology in devices such as cellphones, PDAs, and pagers where optimizing energy consumption is critical. Since, traditionally, the Java virtual machine (JVM), the cornerstone of Java technology, is tuned for performance, taking into account energy consumption requires reevaluation, and possibly redesign of t ...

Keywords: Garbage collector, Java Virtual Machine (JVM), K Virtual Machine (KVM), low power computing

19 Viewpoint: who holds the keys?
William H. Murray
July 1992 **Communications of the ACM**, Volume 35 Issue 7
Publisher: ACM Press
Full text available: pdf(321.27 KB) Additional Information: full citation, index terms

20 Oblivious transfer and polynomial evaluation
Moni Naor, Benny Pinkas
May 1999 **Proceedings of the thirty-first annual ACM symposium on Theory of computing**
Publisher: ACM Press
Full text available: pdf(956.48 KB) Additional Information: full citation, references, citings, index terms

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next